AF JFW

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Alan Boate; Brian Reed	Confirmation No.	7111
Serial No.:	09/775,205		
Filed:	February 1, 2001	Customer No.:	32692
Examiner:	Eleni A. Shiferaw		
Group Art Unit:	2136		
Docket No.:	58057US002 (1004-118US01)		
Title:	METHOD AND SYSTEM FOR SECURING A COMPUTER NETWORK AND PERSONAL IDENTIFICATION DEVICE USED THEREIN FOR CONTROLLING ACCESS TO NETWORK COMPUTERS		

CERTIFICATE UNDER 37 CFR 1.8: I hereby certify that this correspondence is being deposited with the United States Post Service, as First Class Mail, in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450 on January 9, 2007.

By: Patricia Cygan
Name: Patricia Cygan

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
Alexandria, VA 22313-1450

Sir:

We are transmitting herewith the attached correspondence relating to this application:

☒ Transmittal sheet containing Certificate of Mailing
☒ Brief on Appeal in triplicate (37 pgs.)
☒ Fee in the amount of $500.00 to be charged to Deposit Acccount No. 50-1778.
☒ Return postcard

Please apply any charges not covered, or any credits, to Deposit Account No. 50-1778.

Date:
January 9, 2007

By:
Name: Kent J. Sieffert
Reg. No.: 41,312

SHUMAKER & SIEFFERT, P.A.
8425 Seasons Parkway, Suite 105
St. Paul, Minnesota 55125
Telephone: 651.735.1100
Facsimile: 651.735.1102

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Alan Boate; Brian Reed	Confirmation No.	7111
Serial No.:	09/775,205		
Filed:	February 1, 2001	Customer No.:	32692
Examiner:	Eleni A. Shiferaw		
Group Art Unit:	2136		
Docket No.:	58057US002 (1004-118US01)		
Title:	METHOD AND SYSTEM FOR SECURING A COMPUTER NETWORK AND PERSONAL IDENTIFICATION DEVICE USED THEREIN FOR CONTROLLING ACCESS TO NETWORK COMPUTERS		

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
Alexandria, VA 22313-1450

Sir:

This is a Brief on Appeal from the final Office Action mailed on August 9, 2006. A Notice of Appeal was filed on November 9, 2006. Appellant submits this Brief in triplicate. Please charge our Deposit Account No. 50-1778 in the amount of $500.00 to cover the required fee for filing this Brief. Please also charge any additional fees that may be required or credit any overpayment to Deposit Account No. 50-1778.

TABLE OF CONTENTS

REAL PARTY OF INTEREST

The real party of interest is 3M Innovative Properties Company, of St. Paul, Minnesota.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

STATUS OF CLAIMS

Claims 1-21 are on appeal in this case.

Claims 1-21 stand rejected under 35 U.S.C. 103(a) as being anticipated by U.S. Patent No. 6,484,260 to Scott et al. in view of U.S. Patent No. 5,568,552 to Davis, U.S. Patent Application 2002/0191765 to Labaton and U.S. Patent No. 6,594,762 to Doub et al.

STATUS OF AMENDMENTS

No amendments have been filed subsequent to the Final Office Action mailed August 9, 2006 from which this appeal was made.

SUMMARY OF THE INVENTION

Set forth below is a concise summary of independent claim 1, 9 and 17 in reference to the specification and figures via footnotes.

Claim 1

Independent claim 1 is directed to a personal digital identifier device for controlling access to a computer network. Claim 1 requires that the personal digital identifier device (PID) be lightweight and configured for wearing and/or carrying by a user registered and include a wireless communications component comprising a transceiver for communicating with a base unit. Figure 2 of the present application illustrates a wireless transceiver 15[1] of personal identification device (PID) 10 for communicating with base unit 50.[2,3]

Claim 1 also requires that the PID include a biometric acquisition component for obtaining a user's input biometric and producing a digital representation thereof. The present application describes PID 10 as having a biometric acquisition component 35 for acquiring an image of a users fingertip and converting the digital representation to a template.[4,5]

Claim 1 also requires that the PID include a processor configured for communicating with said transceiver and said biometric component and operable for each of the following functions. The present application describes PID 10 as having a microprocessor 20[6] that manages communications between PID 10 and base unit 50, and performs other functions of PID 10.[7]

Claim 1 requires that the processor is operable for evaluating whether a template derived from said digital representation corresponds to a master template derived from a user's biometric digital representation previously produced by said biometric component and generating a matching signal when such a correspondence is determined. The present application describes microprocessor 20 of PID 10 as attempting to match the template to a master template stored in secure memory 25 of PID 10 when the user registered with the system.[8]

Claim 1 requires that the processor is also configured for generating said private key held by said personal digital identifier device and said public key corresponding thereto and outputting said generated public key for transmission by said transceiver. The present application describes microprocessor 20 as generating and internally storing the one or more

[1] Application, e.g., element 15 of Figure 2.
[2] Application, e.g., Paragraphs [0027], [0028] and [0029].
[3] Application, e.g., element 10 and 50 of Figure 1.
[4] Application, e.g., Paragraphs [0027] and [0032].
[5] Application, e.g., element 35 of Figure 2.
[6] Application, e.g., element 20 of Figure 2.
[7] Application, e.g., Paragraphs [0027] and [0028].
[8] Application, e.g., Paragraph [0032].

private and public keys.[9] Only the public key is forwarded to central server 300 and stored in the RA database 360.[10]

Claim 1 requires that the processor is further configured for producing a digital signature using said private key. Microprocessor 20 is provided to create and validate digital signatures for authentication with the private key.[11] In addition, claim 1 requires that the processor is configured for verifying, using said public key for said private key associated with said security manager component, that the source of an encrypted message received from said security manager is said security manager component. The present application describes PID 10 as first authenticating the security manager as the source of messages received from it using an on-board public key of the security manager.[12,13]

Claim 1 also requires secure storage containing said master template of a user's biometric, said generated private key and said public key for said private key associated with said security manager component. According to the present application, the secure storage of the PID device stores the biometric template, which is not transferred to any external component of the system.[14] The present application states that, in addition, private and public keys are held in the secure storage.[15]

Claim 1 also requires a power source and a housing. According to the present application, PID 10 includes battery 40 and a housing that co-operates with a device housing.[16,17]

Additionally, claim 1 requires said personal digital identifier device being configured for producing, using said generated private key, a digitally signed challenge response message following said generating of said matching signal in response to a challenge message received from said security manager component and for transmitting said response message, and said personal digital identifier device being configured to prevent transmission of any of said master

[9] Application, e.g., Paragraphs [0036] and [0037].
[10] Application, e.g., Paragraph [0036].
[11] Application, e.g., Paragraph [0039].
[12] Application, e.g., Paragraph [0030], [0036] and [0037].
[13] Application, e.g., element 40 of Figure 2.
[14] Application, e.g., Paragraph [0036].
[15] Id.
[16] Application, e.g., Paragraph [0027].
[17] Application, e.g., element 40 of Figure 2.

template of a user's biometric and said private key. The present application describes PID 10 as also including a cryptographic software component which manages the creation of one or more public/private key pairs within the PID 10.[18] The authenticity of the PID 10 is confirmed through a communications protocol whereby an on-board (i.e. contained within the PID) private key is used to digitally sign a challenge sent to the PID by the security manager component.[19] Secure storage 25 of PID 10 is provided to securely store only cryptographic keys and the user's biometric template.[20]

Additionally, claim 1 requires that during a currently logged-in session of the user associated with the personal digital identifier device, a policy manager component directs at least one of the workstations to blank out a respective screen when a second personal digital identifier device is detected at a location within an envelope until such time as a user registered to said second personal digital identifier device is biometrically identified to have permission to view data of the currently logged-in session. In relevant part, the present application states that, depending upon the policy manager settings, any sensitive information currently displayed on the screen as part of an existing logged-in session is automatically blanked when a new PID 10 is detected by base unit 50. According to the present application, the screen is not restored until the user of the newly detected PID device has biometrically authenticated themselves with the security manager and the policy manager has determined that they have the right to view this data as an observer.[21]

Claim 9

Independent claim 9 requires a personal digital identifier device that includes a wireless communications component comprising a transceiver. Figure 2 illustrates wireless transceiver 15[22] of personal identification device (PID) 10 for communicating with base unit 50.[23,24] Claim 9

[18] Application, e.g., Paragraph [0030].
[19] Id.
[20] Application, e.g., Paragraph [0027].
[21] Application, e.g., Paragraphs [0033] and [0039].
[22] Application, e.g., element 15 of Figure 2.
[23] Application, e.g., Paragraphs [0027], [0028] and [0029].
[24] Application, e.g., element 10 and 50 of Figure 1.

also requires a biometric acquisition component for obtaining a user's input biometric and producing a digital representation thereof. The present application states that PID 10 includes biometric acquisition component 35 for acquiring an image of a users fingertip and converting the digital representation to a template.[25,26] Claim 9 also requires a processor configured for communicating with said transceiver and said biometric component and operable for the following functions. The present application states that microprocessor 20[27] manages communications between PID 10 and base unit 50, and performs other functions of PID 10.[28]

According to claim 9, the processor is configured for evaluating whether a template derived from said digital representation corresponds to a master template derived from a user's biometric digital representation previously produced by said biometric component and generating a matching signal when such a correspondence is determined. The present application states that microprocessor 20 tries to match the template to a master template stored in secure memory 25 of PID 10 when the user registered with the system.[29]

Claim 9 requires that the processor is configured for generating a private key to be held by said personal digital identifier device and a public key corresponding thereto and outputting said generated public key for transmission by said transceiver. The present application states that microprocessor 20 generates and internally stores the one or more private and public keys.[30] The public key is forwarded to central server 300 and stored in the RA database 360.[31]

Claim 9 also requires that the processor is also configured for producing a digital signature using said private key. The present application states that microprocessor 20 is provided to create and validate digital signatures for authentication with the private key.[32] Additionally, claim 9 requires that the processor is configured for verifying that an encrypted received message is from a security manager component using a public key for a private key

[25] Application, e.g., Paragraphs [0027] and [0032].
[26] Application, e.g., element 35 of Figure 2.
[27] Application, e.g., element 20 of Figure 2.
[28] Application, e.g., Paragraphs [0027] and [0028].
[29] Application, e.g., Paragraph [0032].
[30] Application, e.g., Paragraphs [0036] and [0037].
[31] Application, e.g., Paragraph [0036].
[32] Application, e.g., Paragraph [0039].

associated with said security manager component. PID 10 first authenticates the security manager as the source of messages received from it using an on-board public key of the security manager.[33,34]

Claim 9 also requires secure storage containing said master template of a user's biometric, said generated private key and said public key for said private key associated with said security manager component. The present application describes the secure storage of the PID device as storing the biometric template, which is not transferred to any external component of the system.[35] In addition, private and public keys are held in the secure storage.[36]

Claim 9 also requires said personal digital identifier device being configured for producing, using said generated private key, a digitally signed challenge response message following said generating of said matching signal in response to a challenge received from said security manager component and for transmitting said response message, and said personal digital identifier device being configured to prevent transmission of any of said master template of a user's biometric and said private key. The present application describes each PID 10 as also including a cryptographic software component which manages the creation of one or more public/private key pairs within the PID 10.[37] The authenticity of the PID 10 is confirmed through a communications protocol whereby an on-board (i.e. contained within the PID) private key is used to digitally sign a challenge sent to the PID by the security manager component.[38] Secure storage 25 of PID 10 is provided to securely store only cryptographic keys and the user's biometric template.[39]

Claim 9 requires a base unit associated with said workstation and configured for initiating and maintaining wireless communications with said personal digital identifier device, said communications extending over an area defined by an envelope associated with said workstation, wherein a policy manager component directs the workstation to blank out the screen when a

[33] Application, e.g., Paragraph [0030], [0036] and [0037].
[34] Application, e.g., element 40 of Figure 2.
[35] Application, e.g., Paragraph [0036].
[36] Id.
[37] Application, e.g., Paragraph [0030].
[38] Id.
[39] Application, e.g., Paragraph [0027].

second personal digital identifier device is detected at a location within said envelope until such time as a user registered to said second personal digital identifier device is biometrically identified. The present application states that, depending upon the policy manager settings, any sensitive information currently displayed on the screen as part of an existing logged-in session is automatically blanked when a new PID 10 is detected by base unit 50. The screen is not restored until the user of the newly detected PID device has biometrically authenticated themselves with the security manager and the policy manager has determined that they have the right to view this data as an observer.[40]

Additionally, claim 9 requires a central server having access to network storage and utilizing said security manager component and said personal digital identifier device for authenticating said user, said network storage containing a public key corresponding to said private key generated by said personal digital identifier device. The present application describes a central server 300 stores public keys in PA database 360, and the security manager 340 directs all actions involving cryptography and digital signatures.[41]

Claim 17

Independent claim 17 is directed to a method for controlling access to a computer network in which workstations provide points of access to said network, said network including a central server communicating with said workstations and secure network storage, and a base unit configured for initiating and maintaining wireless communications with a portable personal digital identifier device carried or held by a user being associated with each said workstation, said wireless communications extending over an area defined by an envelope associated with said workstation.

Claim 17 requires that, within said first portable personal digital identifier device, the steps of: receiving an input biometric of said user, producing a digital representation thereof, deriving from said digital representation a master template, securely maintaining said master template in storage, generating and securely maintaining in said storage a private key, generating

[40] Application, e.g., Paragraphs [0033] and [0039].

[41] Application, e.g., Paragraphs [0026], [0030] and [0036].

a public key corresponding to said generated private key and providing said generated public key for storage in said network storage and receiving and storing in said storage a public key for a private key associated with a network security manager component. The present application states that PID 10 includes biometric acquisition component 35 for acquiring an image of a users fingertip and converting the digital representation to a template.[42,43] The secure storage of the PID device stores the biometric template, which is not transferred to any external component of the system.[44] In addition, private and public keys are held in the secure storage.[45] Microprocessor 20 attempts to match the template to a master template stored in secure memory 25 of PID 10 when the user registered with the system.[46] Microprocessor 20 generates and internally stores the one or more private and public keys.[47] The public key is forwarded to central server 300 and stored in the RA database 360.[48]

Claim 17 also requires transmitting a first signal from a base unit associated with one said workstation to said first personal digital identifier device and automatically transmitting from said first personal digital identifier device a response signal establishing communications between said base unit and said first personal digital identifier device in response to said first signal when said first personal digital identifier device is within said envelope. Figure 2 illustrates wireless transceiver 15[49] of personal identification device (PID) 10 for communicating with base unit 50 when the PID is within an envelope associated with base unit 50.[50,51]

Further, claim 17 requires receiving, at said first personal digital identifier device, a digitally signed challenge message from said network security manager component and verifying within said first personal digital identifier device the origin of said challenge using said public key for said private key associated with said security manager component. Each PID 10 also

[42] Application, e.g., Paragraphs [0027] and [0032].
[43] Application, e.g., element 35 of Figure 2.
[44] Application, e.g., Paragraph [0036].
[45] Id.
[46] Application, e.g., Paragraph [0032].
[47] Application, e.g., Paragraphs [0036] and [0037].
[48] Application, e.g., Paragraph [0036].
[49] Application, e.g., element 15 of Figure 2.
[50] Application, e.g., Paragraphs [0027], [0028] and [0029].
[51] Application, e.g., element 10 and 50 of Figure 1.

includes a cryptographic software component that performs the steps of managing the creation of one or more public/private key pairs within the PID 10.[52] The authenticity of the PID 10 is confirmed through a communications protocol whereby an on-board (i.e. contained within the PID) private key is used to digitally sign a challenge sent to the PID by the security manager component.[53]

Claim 17 also requires acquiring on said first portable personal digital identifier device an input biometric of said user, producing a digital representation thereof and deriving from said digital representation a biometric template. The method also includes evaluating within said first portable personal digital identifier device whether said biometric template corresponds to said master template and generating a matching signal when such a correspondence is determined. According to the present application, PID 10 includes biometric acquisition component 35 for acquiring an image of a users fingertip and converting the digital representation to a template.[54,55] Microprocessor 20 tries to match the template to a master template stored in secure memory 25 of PID 10 when the user registered with the system.[56]

In addition, the method of claim 17 requires producing within said first personal digital identifier device, using said generated private key, a digitally signed challenge response message following said generating of said matching signal in response to said challenge message and transmitting said response message to said security manager component to authenticate said first user. According to the present application, each PID 10 also includes a cryptographic software component which manages the creation of one or more public/private key pairs within the PID 10.[57] The authenticity of the PID 10 is confirmed through a communications protocol whereby an on-board (i.e. contained within the PID) private key is used to digitally sign a challenge sent to the PID by the security manager component.[58]

[52] Application, e.g., Paragraph [0030].
[53] Id.
[54] Application, e.g., Paragraphs [0027] and [0032].
[55] Application, e.g., element 35 of Figure 2.
[56] Application, e.g., Paragraph [0032].
[57] Application, e.g., Paragraph [0030].
[58] Id.

The method of claim 17 also requires permitting said authenticated first user to access said computer network through said workstation. An authenticated PID 10 allows the user to be permitted to access the network through the PC 100.[59]

Additionally, claim 17 requires during a currently logged-in session of the first user associated the first personal digital identifier device, directing the workstation to blank out the screen by a policy manager component when a second personal digital identifier device is detected at a location within said envelope until such time as a second user registered to said second personal digital identifier device is biometrically identified to have permission to view data of the currently logged-in session. According to the present application, depending upon the policy manager settings, any sensitive information currently displayed on the screen as part of an existing logged-in session is automatically blanked when a new PID 10 is detected by base unit 50. The screen is not restored until the user of the newly detected PID device has biometrically authenticated themselves with the security manager and the policy manager has determined that they have the right to view this data as an observer.[60]

[59] Application, e.g., Paragraph [0024] and [0026].

[60] Application, e.g., Paragraphs [0033] and [0039].

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

For purposes of this Appeal, Appellants respectfully request review of the rejection of claims 1-21 under 35 U.S.C. 103(a) as being anticipated by U.S. Patent No. 6,484,260 to Scott et al. in view of U.S. Patent No. 5,568,552 to Davis, U.S. Patent Application 2002/0191765 to Labaton and U.S. Patent No. 6,594,762 to Doub et al.

ARGUMENTS OF THE APPELLANT

The First Ground of Rejection

Claims 1-21 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Scott et al. (US 6,484,260) in view of Davis (US 5,568,552), Labaton (US 2002/0191765) and Doub et al. (US 6,594,762).

As summarized above, the Appellant's claimed invention is directed to a network security system and personal digital identifier device (PID) to provide real time authentication of both a person's identity and presence at a computer workstation. The system utilizes a biometric acquisition system to create a digital representation of the user and corresponding master template that is stored within the PID. The PID also generates public and private keys which are used to authenticate the user such that the user may access a workstation and network server.

In addition, the PID may be used to prevent unauthorized users from viewing sensitive information displayed on a workstation. Specifically, the system may blank a display of a currently logged-in session of an authorized user associated with a first device when a second device is detected.[61] In other words, during an active session of an authorized user, the system takes action to blank the screen upon detecting a second device until the second device can be authenticated.

Claim 1

Claim 1 recites a personal digital identifier device for controlling access to a computer network. Claim 1 requires that the personal digital identifier device includes a processor for generating said private key held by said personal digital identifier device and said public key corresponding thereto and outputting said generated public key for transmission by said transceiver. In addition, claim 1 requires a policy manager component of the personal digital identifier device directs at least one of the workstations to blank out a respective screen when a

[61] Application, e.g., Paragraphs [0033] and [0039].

second personal digital identifier device is detected at a location within an envelope until such time as a user registered to said second personal digital identifier device is biometrically identified to have permission to view data of the currently logged-in session.

Contrary to the assertion of the Examiner, Scott in view of Davis, Labaton, and Doub fail to teach or suggest a policy manager component that, during a currently logged-in session of the user associated with the personal digital identifier device, directs at least one of the workstations to blank out a respective screen when a second personal digital identifier device is detected at a location within an envelope until such time as a user registered to said second personal digital identifier device is biometrically identified to have permission to view data of the currently logged-in session.

In rejecting claim 1, the Examiner correctly recognized that Scott in view of Davis and Labaton failed to teach or suggest these elements. In particular, the Examiner admitted that Scott only discloses a user of a personal digital identifier (PID) approaching an ATM and being authenticated to access his or her information.[62] The Examiner then further admitted that Scott in view of Davis and Labaton failed to teach or suggest a policy manager component that directs the workstation to blank out the screen during a currently logged-in session of the user associated with a first personal digital identifier device when a second personal digital identifier device is detected at a location within an envelope until such time as the user registered to the second personal digital identifier device is biometrically identified.

However, the Examiner asserted that Daub teaches these elements and is an obvious combination to Scott in view of Davis and Labaton. In particular, the Examiner stated that "Doub et al. discloses a method of wireless authorized remote device 110 authentication in a range distance proximity and a method of denying a display access of personal data/sensitive data to authorized remote device while the authorized remote device is in logged-in session and away from the computer."[63] For support, the Examiner cited col. 1, ll. 12-35, FIG. 1 and col. 4, ll. 26-45 of Doub.

[62] Office Action dated August 9, 2006, page 10.
[63] Office Action dated August 9, 2006, page 10.

The Examiner's conclusion of obviousness is erroneous for a number of reasons. First, the Examiner's own characterization of Doub reveals that Doub fails to teach Applicant's claim elements that the Examiner previously admitted are not taught by the other references. The Examiner admitted that Scott in view of Davis and Labaton failed to teach or suggest a policy manager component that performs the function of actively blanking a workstation screen during a currently logged-in session of an authorized user when a second personal digital identifier device is detected until such time as the user registered to the second personal digital identifier device is also biometrically identified. In contrast, the Examiner characterized Doub as disclosing only "a method of denying a display access of personal data/sensitive data to authorized remote device while the authorized remote device is in logged-in session and away from the computer."

Notably, the Examiner's characterization of Doub makes no reference to detection of a second device at all, let alone during a currently logged-in session of an authorized user associated with a first device. Moreover, the Examiner's characterization of Doub only refers to denying a display access when that authorized user is away from the computer. This is inadequate to teach or discuss detecing the presence of a second PID while a first PID is currently logged-in and then actively blanking a display of the currently logged-in session of the authorized user associated with a first device when the second device is detected. This is prima facie evidence of the deficiency of Doub as teaching such elements.

This inadequacy is borne out in the disclosure of Doub, which only describes "enabling a display of an electronic device when the electronic device and a remote device, are located within a transmit range of each other and disabling the display when the electronic device and the remote device are not within the transmit range of each other."[64] Doub makes very clear that disabling of the display only occurs when the electronic device and the remote device are out of transmit range of each other.

Disabling a display when no authorized device is in range, as taught by Doubs, does not provide any basis for blanking a display of a currently logged-in session of an authorized user

[64] Doub et al., col. 1, ll. 48-52.

associated with a first device when a second device is detected, i.e., within range. Quite the contrary, the Doub system teaches handling the situation quite differently.

According to Doub, a screen is only blanked when the currently authorized device is no longer in range. If the device of the authorized user is within range, according to the teachings of Doub, the Doub system does not disable the screen. This entirely contradicts Applicant's claim language. For at least this reason, even if one of ordinary skill were motivated to combine Scott in view of Davis and Labaton with the teachings of Daub, the resulting system would not include a policy manager component that directs at least one of the workstations to blank out a respective screen of a currently logged-in session of an authorized user when a second personal digital identifier device is detected at a location within an envelope.

Doub does contemplate or discuss the situation where an unauthorized, or second, remote device is detected during a session of an authorized user. Doub explains that "the first authentication code may provide additional security against an unauthorized remote device masquerading as the authorized remote device 110."[65] Doub continues, "If the reply signal does not include the correct first authentication code, the display controller 210 will not enable the display 115."[66] Doub only states that controller 210 will not enable display 115 if the remote device is unauthorized. This, therefore, refers to the situation where the display is already disabled and the only device that responds is an unauthorized device. However, Doub does not contemplate the situation where multiple devices are present, where one of the devices relates to an authorized user that is already logged-in, and a second device is detected that is associated with a user that has not yet authorized.

The Examiner has pointed to no teaching in any of the references, even in combination, that suggest handling the situation where multiple devices are present, one of the devices relates to an authorized user that is already logged-in, and a second device is associated with a user that has not yet authorized. The combination proposed by the Examiner would not result in a system that blanks out a screen of a logged-in session of an authorized user when a second personal digital identifier device is detected, as required by the independent claims. Instead, the teachings

[65] Doub et al., Col. 4, ll. 38-40.
[66] Doub et al., Col. 4, ll. 41-43.

pointed to by the Examiner suggest that the system would enable the screen in this case since the first device is an authorized device and, presumably, within transmit range. In fact, the system suggested by the Examiner would not take any action until the first device is no longer in transmit range, which fails to teach or suggest the features of claim 1.

Further, the cited references fail to teach or suggest a personal digital identifier that internally generates and stores a private key and a public for encrypted communications. Specifically, with respect to claim 1, the cited references fail to teach or suggest a personal digital identifier have a processor for generating said private key held by said personal digital identifier device and said public key corresponding thereto and outputting said generated public key for transmission by said transceiver, as required by claim 1. In the Office Action at pg. 8, the Examiner cited Scott as anticipating teaching a personal digital identifier device having these elements, i.e., a PID capable of internally generating both a private key and a public key. However, the Examiner is misinterpreting the Scott disclosure. In fact, Scott directly states that "The private encryption key is stored or loaded into PID 6 at registration time or at manufacture."[67]

Therefore, the Scott system relied on by the Examiner is in direct contrast to the claim 1. The Examiner overlooked and failed to address the fact that Scott does not teach or provide motivation to generate the private key as well as the public key on the portable device itself. Without pointing to any teaching or motivation to do so within the evidentiary record, programming the master template into the PID, as taught by Scott, does not teach or suggest a PID capable of internally generating both the private and public keys. Appellant has recognized the possible advantages of locally generating a public and private keys for the portable identification device without requiring a master biometric template or the keys be transmitted or programmed into the device. Scott in view of the other references does not recognize nor teach these features.

For at least these reasons, Scott in view of Davis, Labaton, and Doub all fail to suggest the elements of claim 1. The Examiner has failed to provide motivation within the evidentiary

[67] Scott et al., Col. 10, ll. 50-52.

record that would cause someone of ordinary skill in the art to duplicate the elements of claim 1. For at least these reasons, the rejection of claim 1 improper and needs to be reversed.

Claim 9

Claim 9 recites a security system for controlling access to a computer network at a network access point comprising a workstation. The system of claim 9 requires a personal digital identifier device, a base unit, and a central server. The personal digital identifier device includes a processor configured for generating a private key to be held by said personal digital identifier device and a public key corresponding thereto and outputting said generated public key for transmission by said transceiver. The base unit is associated with a workstation and configured for initiating and maintaining wireless communications with said personal digital identifier device, said communications extending over an area defined by an envelope associated with said workstation. A policy manager component directs the workstation to blank out the screen when a second personal digital identifier device is detected at a location within said envelope until such time as a user registered to said second personal digital identifier device is biometrically identified.

As discussed with reference to claim 1, Scott in view of Davis, Labaton, and Doub fail to teach or suggest a policy manager component that directs the workstation to blank out the screen when a second personal digital identifier device is detected at a location within said envelope until such time as a user registered to said second personal digital identifier device is biometrically identified.

Again, the Examiner's own characterization of Doub does not teach Applicant's claim elements that the Examiner previously admitted are not taught by the other references. The Examiner admitted that Scott in view of Davis and Labaton failed to teach or suggest a policy manager component that performs the function of actively blanking a workstation screen even during a currently logged-in session of an authorized user when a second personal digital identifier device is detected until such time as the user registered to the second personal digital identifier device is also biometrically identified. In contrast, the Examiner characterized Doub as disclosing only "a method of denying a display access of personal data/sensitive data to authorized remote device while the authorized remote device is in logged-in session and away from the computer."

Notably, the Examiner's characterization of Doub makes no reference to detection of a second device at all, let alone during a currently logged-in session of an authorized user associated with a first device. Moreover, the Examiner's characterization of Doub only refers to denying a display access when that authorized user is away from the computer.

Further, as discussed above with respect to claim 1, Scott in view of the other refences fails to teach or suggest a processor for generating said private key held by said personal digital identifier device and said public key corresponding thereto and outputting said generated public key for transmission by said transceiver, as required by claim 9. Moreover, Scott in view of the other references fail to teach or suggest a personal digital identifier device that is configured to prevent transmission of any of said master template of a user's biometric and the private key, as specifically required by claim 9

The Examiner cited Scott as anticipating that the personal digital identifier device includes a processor for generating the private key held by said personal digital identifier device. The Examiner is misinterpreting the Scott disclosure. Scott directly states that "The private encryption key is stored or loaded into PID 6 at registration time or at manufacture."[68]

The Scott system is in direct contrast to the claim 9. The Examiner overlooked and failed to address the fact that Scott does not teach or provide motivation to generate the master template on the portable device itself. In fact, nowhere within the disclosure does Scott describe where the master template is generated. Storing or loading the master template on the portable device is not equivalent to generating the master template on the portable device without pointing to any teaching or motivation to do so within the evidentiary record. Applicant has recognized the possible advantages of locally generating a master template for a biometric on a portable device without requiring the master biometric template be transmitted to the device. Scott does not recognize nor teach these features, and the teaching and motivation to provide these element of claim 1 cannot be plucked from the Applicant's own disclosure.

[68] Scott et al., Col. 10, ll. 50-52.

For substantially the reasons stated above with respect to claim 1, Scott and Scott in view of Davis, Labaton, and Doub all fail to suggest the requirements of claim 9. For this reason, the final rejection of claim 9 should be reversed.

Claim 13

Dependent claim 13 is dependent upon independent claim 9. Dependent claim 13 is separately patentable from independent claim 9 and does not necessarily stand or fall with independent claim 9.

Dependent claim 13 further requires a plurality of said personal digital identifier devices, a plurality of workstations and a plurality of base units wherein a base unit is associated with each said workstation, each said base unit transmitting a polling signal to each said personal digital identifier device within said base unit's associated envelope following said base unit's receipt of said response signal from each said personal digital identifier device. Contrary to the assertion of the Examiner, Scott, or Scott in combination of any other cited reference, fails to suggest the elements of claim 13.

Scott describes that "a user of PID 6 approaches host facility 4, e.g., an ATM (100). As PID 6 reaches the range of the host facility's receiver module 38, the microprocessor is 'powered up.'"[69] However, there is no disclosure within Scott, or any other references, that motivate one of ordinary skill in the art to transmit a <u>polling signal</u> to said personal digital identifier device for determining whether said personal digital identifier device <u>remains located within</u> said base unit's associated envelope. Accordingly, for this additional reason, the rejection of claim 13 should be reversed.

Claim 16

Dependent claim 16 is dependent upon independent claim 9 and argued separately. Dependent claim 16 is separately patentable from independent claim 9 and does not necessarily stand or fall with independent claim 9.

[69] Scott, Col. 10, ll. 58-61.

Dependent claim 16 further requires that said envelop has a shape and area which are configured to encompass those locations proximate to said workstation at which an observer may read and/or understand information displayed on a screen of said workstation. Contrary to the assertion of the Examiner, both Scott and Doub, fail to suggest the elements of claim 16.

Scott teaches that a "transmitter module includes an induction loop data link, which is configured as a short-range (<0.5 m) wireless modem..."[70] However, any transmitter has a "range" that is not identical to an envelope specifically having a shape and area. Scott does not provide motivation to someone or ordinary skill in the art to duplicate the requirement that the envelope has a shape and area to encompass those locations proximate to said workstation.

Similar to Scott, Doub suggests a transmitter "range." Doub discloses that "the display 115 is enabled when the electronic device 100 and the remote device 110 are located within a transmit range, Rt, of each other."[71] As mentioned above with respect to Scott, any transmitter has a "range" which is not identical to an envelope having a shape and area. Doub fails to provide any motivation to someone of ordinary skill in the art to duplicate the requirements of claim 16.

It is improper for the Examiner to pluck motivation from claim 16 instead of providing motivation from the evidentiary record. Accordingly, for this additional reason, the rejection of claim 16 should be reversed.

[70] Scott, Col. 9, ll. 28-30.
[71] Doub et al., Col. 3, ll. 26-28.

Claim 17

Claim 17 recites a method for controlling access to a computer network in which workstations provide points of access to the network. The method claim 9 requires within said first portable personal digital identifier device: generating and securely maintaining in the storage a private key and generating a public key corresponding to said generated private key. Claim 9 also requires during a currently logged-in session of the first user associated the first personal digital identifier device, directing the workstation to blank out the screen by a policy manager component when a second personal digital identifier device is detected at a location within said envelope until such time as a second user registered to said second personal digital identifier device is biometrically identified to have permission to view data of the currently logged-in session.

As discussed with reference to claims 1 and 9, Scott in view of Davis, Labaton, and Doub fail to teach or suggest directing the workstation to blank out the screen by a policy manager component when a second personal digital identifier device is detected at a location within said envelope until such time as a second user registered to said second personal digital identifier device is biometrically identified to have permission to view data of the currently logged-in session.

Again, the Examiner's own characterization of Doub does not teach Applicant's claim elements that the Examiner previously admitted are not taught by the other references. The Examiner admitted that Scott in view of Davis and Labaton failed to teach or suggest a policy manager component that performs the function of actively blanking a workstation screen even during a currently logged-in session of an authorized user when a second personal digital identifier device is detected until such time as the user registered to the second personal digital identifier device is also biometrically identified. In contrast, the Examiner characterized Doub as disclosing only "a method of denying a display access of personal data/sensitive data to authorized remote device while the authorized remote device is in logged-in session and away from the computer."

Notably, the Examiner's characterization of Doub makes no reference to detection of a second device at all, let alone during a currently logged-in session of an authorized user associated with a first device. Moreover, the Examiner's characterization of Doub only refers to denying a display access when that authorized user is away from the computer.

Further, as discussed above with respect to claims 1 and 9, Scott fails to teach or suggest within the personal digital identifier device: generating said private key held by said personal digital identifier device and said public key corresponding thereto and outputting said generated public key for transmission by said transceiver, as required by claim 17.

The Examiner cited Scott as anticipating that the personal digital identifier device includes a processor for generating the private key held by said personal digital identifier device. The Examiner is misinterpreting the Scott disclosure. Scott directly states that "The private encryption key is stored or loaded into PID 6 at registration time or at manufacture."[72]

The Scott system is in direct contrast to the claim 17. The Examiner overlooked and failed to address the fact that Scott does not teach or provide motivation to generate the master template on the portable device itself. In fact, nowhere within the disclosure does Scott describe where the master template is generated. Storing or loading the master template on the portable device is not equivalent to generating the master template on the portable device without pointing to any teaching or motivation to do so within the evidentiary record. Applicant has recognized the possible advantages of locally generating a master template for a biometric on a portable device without requiring the master biometric template be transmitted to the device. Scott does not recognize nor teach these features, and the teaching and motivation to provide these element of claim 1 cannot be plucked from the Applicant's own disclosure.

For substantially the reasons stated above with respect to claims 1 and 9, Scott and Scott in view of Davis, Labaton, and Doub all fail to suggest the requirements of claim 17. For this reason, the final rejection of claim 17 should be reversed.

[72] Scott et al., Col. 10, ll. 50-52.

Claim 18

Dependent claim 18 is dependent upon independent claim 17 and argued separately. Dependent claim 18 is separately patentable from independent claim 17 and does not necessarily stand or fall with independent claim 17.

Dependent claim 18 further requires configuring the shape and area of said envelope to encompass those locations proximate to said workstation at which an observer may read and/or understand 'information displayed on a screen of said workstation. Contrary to the assertion of the Examiner, both Scott and Doub, fail to suggest the elements of claim 18.

As discussed above with respect to claim 16, Scott teaches that a "transmitter module includes an induction loop data link, which is configured as a short-range (<0.5 m) wireless modem..."[73] However, any transmitter has a "range" that is not identical to an envelope specifically having a <u>shape and area</u>. Scott does not provide motivation to someone or ordinary skill in the art to duplicate the requirement that the envelope has a shape and area to encompass those locations proximate to said workstation.

In addition, Doub suggests a transmitter "range." Doub discloses that "the display 115 is enabled when the electronic device 100 and the remote device 110 are located within a transmit range, Rt, of each other."[74] As mentioned above with respect to Scott, any transmitter has a "range" which is not identical to an envelope having a <u>shape and area</u>. Doub fails to provide any motivation to someone of ordinary skill in the art to duplicate the requirements of claim 18.

It is improper for the Examiner to pluck motivation from claim 18 instead of providing motivation from the evidentiary record. Accordingly, for this additional reason, the rejection of claim 18 should be reversed.

Claim 19

Dependent claim 19 is dependent upon independent claim 17 and argued separately. Dependent claim 19 is separately patentable from independent claim 17 and does not necessarily stand or fall with independent claim 17.

[73] Scott, Col. 9, ll. 28-30.

[74] Doub et al., Col. 3, ll. 26-28.

Dependent claim 19 further requires following said base unit's receipt of said response signal from said personal digital identifier device, transmitting from said base unit a polling signal to said personal digital identifier device for determining whether said personal digital identifier device remains located within said base unit's associated envelope. Contrary to the assertion of the Examiner, Scott, or Scott in combination of any other cited reference, fails to suggest the elements of claim 19.

As mentioned above with respect to claim 13, Scott describes that "a user of PID 6 approaches host facility 4, e.g., an ATM (100). As PID 6 reaches the range of the host facility's receiver module 38, the microprocessor is 'powered up.'"[75] However, there is no disclosure within Scott, or any other references, that motivate one of ordinary skill in the art to transmit a polling signal to said personal digital identifier device for determining whether said personal digital identifier device remains located within said base unit's associated envelope. Accordingly, for this additional reason, the rejection of claim 19 should be reversed.

Claim 21

Dependent claim 21 is dependent upon independent claim 17 and argued separately. Dependent claim 21 is separately patentable from independent claim 17 and does not necessarily stand or fall with independent claim 17.

Dependent claim 21 further requires initially registering said user by a registrar in the presence of a guarantor, said registrar and guarantor each being a registered user of the computer network and said registrar having access to the computer network and verified by said security manager component to have registration privileges, and requiring: that said guarantor provide to said security manager component a biometrically digitally signed message to authenticate said guarantor and that each of said registrar, guarantor and user remain within said envelope during said registering of said user. Contrary to the assertion of the Examiner, Scott, or Scott in combination of any other cited reference, fails to suggest the elements of claim 21.

[75] Scott, Col. 10, ll. 58-61.

Scott discloses that "the users register by presenting themselves with their PID 6 and the required personal identification papers, which is no different than current methods of obtaining a bank card to access accounts with an ATM."[76] However, there is no teaching that suggests that each of said registrar, guarantor and user remain within said envelope during said registering of said user. The Examiner has not provided any motivation within the evidentiary record that would allow someone of ordinary skill in the art to duplicate the elements of claim 21. Accordingly, for this additional reason, the rejection of claim 21 should be reversed.

CONCLUSION OF ARGUMENTS

The final Office Action failed to establish anticipation with respect to claims 1-21. In view of Appellant's arguments, the final rejections of claims 1-21 are improper and should be reversed.

Each of the different claims addressed separately above are separately patentable. Accordingly, the different claims do not necessarily stand or fall together.

Date:

January 9, 2007

SHUMAKER & SIEFFERT, P.A.
8425 Seasons Parkway, Suite 105
St. Paul, Minnesota 55125
Telephone: 651.735.1100
Facsimile: 651.735.1102

By:

Kent J. Sieffert

Name: Kent J. Sieffert
Reg. No.: 41,312

[76] Scott, Col. 11, ll. 47-51.

APPENDIX: CLAIMS ON APPEAL

Claim 1 (Previously Presented): A personal digital identifier device for controlling access to a computer network, said network comprising a plurality of workstations each having a base unit associated therewith, said base unit being configured for wireless communications with said personal digital identifier device, and said network further comprising a central server utilizing a security manager component and network storage, said security manager component associated with a private key and a corresponding public key and said network storage containing a public key corresponding to a private key held by said personal digital identifier device, said personal digital identifier device being lightweight, configured for wearing and/or carrying by a user registered thereto and comprising:

(a) a wireless communications component comprising a transceiver for communicating with said base unit;

(b) a biometric acquisition component for obtaining a user's input biometric and producing a digital representation thereof;

(c) a processor configured for communicating with said transceiver and said biometric component and operable for:

(i) evaluating whether a template derived from said digital representation corresponds to a master template derived from a user's biometric digital representation previously produced by said biometric component and generating a matching signal when such a correspondence is determined;

(ii) generating said private key held by said personal digital identifier device and said public key corresponding thereto and outputting said generated public key for transmission by said transceiver;

(iii) producing a digital signature using said private key; and,

(iv) verifying, using said public key for said private key associated with said security manager component, that the source of an encrypted message ostensibly received from said security manager is said security manager component;

(d) secure storage containing said master template of a user's biometric, said generated private key and said public key for said private key associated with said security manager component;

(e) a power source; and,

(f) a housing,

said personal digital identifier device being configured for producing, using said generated private key, a digitally signed challenge response message following said generating of said matching signal in response to a challenge message received from said security manager component and for transmitting said response message, and said personal digital identifier device being configured to prevent transmission of any of said master template of a user's biometric and said private key,

and wherein, during a currently logged-in session of the user associated with the personal digital identifier device, a policy manager component directs at least one of the workstations to blank out a respective screen when a second personal digital identifier device is detected at a location within an envelope until such time as a user registered to said second personal digital identifier device is biometrically identified to have permission to view data of the currently logged-in session.

Claim 2 (Original): A personal digital identifier device according to claim 1 wherein said biometric component includes a transducer.

Claim 3 (Original): A personal digital identifier device according to claim 1 wherein a response signal is automatically transmitted from said transceiver in response to a signal received by said transceiver from one said base unit.

Claim 4 (Original): A personal digital identifier device according to claim 1 wherein all data held in said secure storage is by itself non-identifiable of said user.

Claim 5 (Original): A personal digital identifier device according to claim 2 wherein said transducer comprises a solid state fingerprint sensor.

Claim 6 (Original): A personal digital identifier device according to claim 5 wherein said transceiver transmits and receives optical signals.

Claim 7 (Original): A personal digital identifier device according to claim 6 wherein said transceiver transmits and receives radio frequency signals.

Claim 8 (Original): A personal digital identifier device according to claim 1 in combination with a device holder wherein said device holder is configured to co-operate with said housing of said personal digital identifier device such that said personal digital identifier device is held by said holder device when it is appropriately positioned relative to said holder device, said device holder comprising a communications connector for communicatively coupling said personal digital identifier device directly to one said workstation when said personal digital identifier device is held by said device holder.

Claim 9 (Previously Presented): A security system for controlling access to a computer network at a network access point comprising a workstation, said system comprising:

A. a personal digital identifier device comprising:

(a) a wireless communications component comprising a transceiver;

(b) a biometric acquisition component for obtaining a user's input biometric and producing a digital representation thereof;

(c) a processor configured for communicating with said transceiver and said biometric component and operable for:

(i) evaluating whether a template derived from said digital representation corresponds to a master template derived from a user's biometric digital representation previously produced by said biometric component and generating a matching signal when such a correspondence is determined;

(ii) generating a private key to be held by said personal digital identifier device and a public key corresponding thereto and outputting said generated public key for transmission by said transceiver;

(iii) producing a digital signature using said private key; and,

(iv) verifying that an encrypted received message is from a security manager component using a public key for a private key associated with said security manager component; and,

(d) secure storage containing said master template of a user's biometric, said generated private key and said public key for said private key associated with said security manager component,

said personal digital identifier device being configured for producing, using said generated private key, a digitally signed challenge response message following said generating of said matching signal in response to a challenge received from said security manager component and for transmitting said response message, and said personal digital identifier device being configured to prevent transmission of any of said master template of a user's biometric and said private key;

B. a base unit associated with said workstation and configured for initiating and maintaining wireless communications with said personal digital identifier device, said communications extending over an area defined by an envelope associated with said workstation, wherein a policy manager component directs the workstation to blank out the screen when a second personal digital identifier device is detected at a location within said envelope until such time as a user registered to said second personal digital identifier device is biometrically identified; and,

C. a central server having access to network storage and utilizing said security manager component and said personal digital identifier device for authenticating said user, said network storage containing a public key corresponding to said private key generated by said personal digital identifier device.

Claim 10 (Original): A security system according to claim 9 wherein said biometric component includes a transducer.

Claim 11 (Original): A security system according to claim 9 wherein said workstation is a personal computer.

Claim 12 (Original): A security system according to claim 9 wherein said base unit regularly transmits a first signal to said personal digital identifier device and said personal digital identifier device automatically transmits a response signal in response thereto when said personal digital identifier device is within said envelope.

Claim 13 (Original): A security system according to claim 12 comprising a plurality of said personal digital identifier devices, a plurality of workstations and a plurality of base units wherein a base unit is associated with each said workstation, each said base unit transmitting a polling signal to each said personal digital identifier device within said base unit's associated envelope following said base unit's receipt of said response signal from each said personal digital identifier device.

Claim 14 (Original): A security system according to claim 9 wherein all data held in said secure storage of said personal digital identifier device is by itself non-identifiable of said user.

Claim 15 (Original): A security system according to claim 9 wherein said network storage includes data identifiable of said user for display on a screen of said workstation when said user's personal identification device is located within said envelope.

Claim 16 (Original): A security system according to claim 9 wherein said envelop has a shape and area which are configured to encompass those locations proximate to said workstation at which an observer may read and/or understand information displayed on a screen of said workstation.

Claim 17 (Previously Presented): A method for controlling access to a computer network in which workstations provide points of access to said network, said network including a central server communicating with said workstations and secure network storage, and a base unit configured for initiating and maintaining wireless communications with a portable personal digital identifier device carried or held by a user being associated with each said workstation, said wireless communications extending over an area defined by an envelope associated with said workstation, said method comprising the steps:

(a) on registration of a first portable personal digital identifier device to a first user, within said first portable personal digital identifier device: receiving an input biometric of said user, producing a digital representation thereof, deriving from said digital representation a master template, securely maintaining said master template in storage, generating and securely maintaining in said storage a private key, generating a public key corresponding to said generated private key and providing said generated public key for storage in said network storage and receiving and storing in said storage a public key for a private key associated with a network security manager component;

(b) transmitting a first signal from a base unit associated with one said workstation to said first personal digital identifier device and automatically transmitting from said first personal digital identifier device a response signal establishing communications between said base unit and said first personal digital identifier device in response to said first signal when said first personal digital identifier device is within said envelope;

(c) receiving at said first personal digital identifier device a digitally signed challenge message ostensibly from said network security manager component and verifying within said first personal digital identifier device the origin of said challenge using said public key for said private key associated with said security manager component;

(d) acquiring on said first portable personal digital identifier device an input biometric of said user, producing a digital representation thereof and deriving from said digital representation a biometric template;

(e) evaluating within said first portable personal digital identifier device whether said biometric template corresponds to said master template and generating a matching signal when such a correspondence is determined;

(f) producing within said first personal digital identifier device, using said generated private key, a digitally signed challenge response message following said generating of said matching signal in response to said challenge message and transmitting said response message to said security manager component to authenticate said first user;

(g) permitting said authenticated first user to access said computer network through said workstation; and

(h) during a currently logged-in session of the first user associated the first personal digital identifier device, directing the workstation to blank out the screen by a policy manager component when a second personal digital identifier device is detected at a location within said envelope until such time as a second user registered to said second personal digital identifier device is biometrically identified to have permission to view data of the currently logged-in session.

Claim 18 (Original): A method according to claim 17 and further comprising configuring the shape and area of said envelope to encompass those locations proximate to said workstation at which an observer may read and/or understand 'information displayed on a screen of said workstation.

Claim 19 (Original): A method according to claim 17 and further comprising, following said base unit's receipt of said response signal from said personal digital identifier device, transmitting from said base unit a polling signal to said personal digital identifier device for determining whether said personal digital identifier device remains located within said base unit's associated envelope.

Claim 20 (Original): A method according to claim 17 and further comprising displaying on a screen of said workstation data identifying said user when said user is identified.

Claim 21 (Original): A method according to claim 17 and further comprising initially registering said user by a registrar in the presence of a guarantor, said registrar and guarantor each being a registered user of the computer network and said registrar having access to the computer network and verified by said security manager component to have registration privileges, and requiring: that said guarantor provide to said security manager component a biometrically digitally signed message to authenticate said guarantor and that each of said registrar, guarantor and user remain within said envelope during said registering of said user.

Claim 22 (Cancelled)

EVIDENCE APPENDIX

NONE

RELATED PROCEEDINGS APPENDIX

NONE